ADDITIONAL SHEET

CCR#: 04-0200 **Rev:** **Originator:** Henry Baez
Telephone: 301-925-1025 **Office:** 3108G
Title of Change: Release of SCP Script file to all DAAC for installation on firewalls.

This delivery contains the script file that will be run on the sites firewall to grep only anonymous FTP associated with Data Pool pulls. The script file will be run every night by a cron entry. The Secure Copy (SCP) will be the method to transfer the file from the firewall to the site x0dps01 host. It order to do this unattended, keys must be exchanged between the firewall and the dps01 host. This exchanged of keys will allow the general user ID that runs the log parser, cmshared in PVC, to get the file.

The script is to be installed on the following machines:

- e0fwi09
- g0fwi09
- l0fwi09
- n0fwi09
- p0fwi09
- t1fwi09

The script was tested successfully between the PVC firewall, p0fwi09 and p2ps01 in the PVC.

INSTALLATION INSTRUCTIONS for SCP Script File

The following provides the installation and configuration procedures to install the SCP script file on the firewall and setting up key exchange.

Prerequisites

1. A directory to put the script is required. In the PVC firewall the /scripts directory was created.

2. Have to generate 1024 bit key on the firewall and exchange keys with the cmshared or allmode account on x0dps01 host.

Uninstall Instructions

1. None.

Installation Instructions

1. The following script is copied or created in /scripts directory:

```
#Purpose: On a daily bases take Data Pool FTP anonyous flows from firewall
#logs and scp them to x0dps01 Data Pool server in B0 network.
#
#Henry Baez
#301-925-1025
#
#Revision History
#=========================
#01/15/2004 - Intial script creation
#01/19/2004 - First draft
#02/17/2004 - Test with cmshared
#02/20/2004 - Grep ftproxy added to get rid of webgate p2dps01 errors
#03/30/2004 - Log file name changed to datapoolftplog
#03/31/2004 - Case st. and 'logrotation' feature
#
#Define Variables (Most DAAC will be /var/adm for LOGDIR for now)
```

```
#But after 3th drive install, it will be /log, as in PVC now
#
TMPDIR="/tmp"
LOGDIR="/log"
SCPDIR="/usr/local/bin"
DPLOGDIR="/usr/ecs/OPS/COTS/firewall/logs"
#
  date +"%b %e" > $TMPDIR/datepool
  day=`date +"%a"`
  sleep 600
#
#Must change the IP address of the site dps01 hosts
  cat $LOGDIR/syslog | grep -f $TMPDIR/datepool | grep "198.118.220.80" | grep f
tproxy > $TMPDIR/datapoolftplog

  case "$day" in
        Sun) $SCPDIR/scp /tmp/datapoolftplog
cmshared@198.118.220.80:$DPLOGDIR/datapoolftplog.0;;
        Mon) $SCPDIR/scp /tmp/datapoolftplog cmshared@198.118.220.80:$DPLOGDIR/d
atapoolftplog.1;;
        Tue) $SCPDIR/scp /tmp/datapoolftplog cmshared@198.118.220.80:$DPLOGDIR/d
atapoolftplog.2;;
        Wed) $SCPDIR/scp /tmp/datapoolftplog cmshared@198.118.220.80:$DPLOGDIR/d
atapoolftplog.3;;
        Thu) $SCPDIR/scp /tmp/datapoolftplog cmshared@198.118.220.80:$DPLOGDIR/d
atapoolftplog.4;;
        Fri) $SCPDIR/scp /tmp/datapoolftplog cmshared@198.118.220.80:$DPLOGDIR/d
atapoolftplog.5;;
        Sat) $SCPDIR/scp /tmp/datapoolftplog cmshared@198.118.220.80:$DPLOGDIR/d
atapoolftplog.6;;
  esac
```

2. At GSFC DAAC the user is allmode, so script has to be changed.

3. The IP address of the sites dps01 host will replace the IP of p2dps01, 198.118.232.80, above.

4. Another changes might be the location of the syslog file. It will be /var/adm at all sites before the installation of the 3rd drive. After the 3rd dive is install it will be /log.

5. An entry similar to the one below must be added to the cron:

   ```
   55 23 * * * /scripts/synergylog
   ```

   The above will run the script at 23:55. First the script gets the month and date and put this to a file. It then gets the abbreviated day of the week and puts this to a variable. It then sleeps for 10 minutes and at 00:05 will use grep to put to a file all anonymous FTP for the month and date to a file. Based on the day of the week, it will copy the log file to x0dps01 and named it with an extension that will have the number 0 to 6 behind it. These numbers represent Sunday through Saturday, like in cron notation.

6. The first step to set up host authentication is to generate a 1024 bit key. During installation of the F-Secure Client SSH binary, the install program generates a 2048 key that does not work.

   a. Run on firewall: /usr/local/bin/ssh-keygen2 –c firewall –t dsa –b 1024 –P (The name firewall is just a label). Root password on firewall needed.

b. On firewall scp the file generated with above command, id_dsa_1024_a.pub, to cmshared (allmode) home directory on dps01 host. Using the command:
scp2 ~/.ssh2/ id_dsa_1024_a.pub
cmshared(allmode)@x0dps01:.ssh2/domains/firewall.pub

This will require someone with the cmshared/allmode password.

c. On firewall in /.ssh2 directory create a file named 'identification' and put in a single line that reads: "IdKey id_dsa_1024_a". Again need firewall root access.

d. On client run the command /usr/local/bin/sshconcat2. This will add a line to the /home/cmshared(or allmode)/.ssh2/authorization file. Need someone with cmshared or allmode account password to do this.

Interrogation Checkout

1. Run script on firewall and make sure you do not need to provide a password and the file'datapoolftplog' with correct extension is the host x0dps01 in the directory /usr/ecs/OPS/COTS/firewall/logs. The extensions are .0 for Sunday, .1 for Monday, .2 for Tuesday, .3 for Wednesday, .4 for Thursday, .5 for Friday, and .6 for Saturday.

Back-Out Instructions

1. Delete the script.
2. Comment out or delete the cron entry.